Tink Germany GmbH Privacy Notice for End Users

Version 6.0: April 2026

Tink Germany GmbH values your trust and respects your privacy. This Privacy Notice for End Users ("**Privacy Notice**") explains how Tink Germany GmbH ("**Tink Germany**", "**we**," "**us**", and/or "**our**") processes your Personal Data, including how we collect, use, and share it, when you use our Services (as defined below), and related services that link to this Privacy Notice. Tink Germany is the controller for the processing of your Personal Data as described in this Privacy Notice if you have agreed to Tink Germany's End-User Terms of Service ("**Terms**").

What is covered by this Privacy Notice?

About Our Services

The open banking platform enables our business partners ("**Partners**") to build services that leverage financial information of individuals ("**End Users**" or "**you**").

We provide account information services ("**AIS**") and payment initiation services ("**PIS**") ("**Services**") to End Users and Partners, which allow End Users to share their financial information with Partners and / or to make payments. We offer PIS in two different forms. These forms are called Pay/OnlineÜberweisen and PayPlus/OnlineÜberweisenPlus. We offer our AIS either for a one-off data retrieval ("**One-off AIS**") or as a continuous connection for recurring data retrieval ("**Continuous AIS**"). We provide our Services through the applications or websites of Partners that offer their own services to you (for example merchants, banks, financial institutions or other service providers). Partners for the purposes of our Terms and this Privacy Notice are

companies that use our Services either under a contract with us or through one of our contractual partners.

When you request services from a Partner, the Partner will integrate our open banking platform, so we can collect your financial information or initiate a payment on your behalf. You might receive our Services differently depending on the type of account(s) you have, and the way your account provider (for example, your bank or card issuer) ("**Account Provider**" **or** "**Bank**") provides access to your account(s).

Scope of this Privacy Notice

When we provide Services directly to End Users, End Users will sign up to our End-User Terms of Service. In this scenario, this Privacy Notice applies to the processing, including the collection, use and sharing of End Users' Personal Data that we process in connection with the provision of the Services.

When we act on behalf of Partners as a data processor, we only collect, use, and share Personal Data as authorized by contracts with Partners. In this scenario, the privacy notice provided by the Partner with which you have a relationship will apply and this Privacy Notice does not apply. This Privacy Notice does not cover what others, such as Partners, websites or other applications, do with your Personal Data. This Privacy Notice also does not cover Personal Data we collect through our websites, or when you interact with our websites. Please read the privacy notices published on our websites or otherwise provided to you when you interact directly with us.

In this Privacy Notice, "**Personal Data**" refers to information that (alone or when used in combination with other information) is capable of being associated with or could reasonably be associated with an individual. The Personal Data we collect varies depending on our relationship and interactions with you.

Categories of Personal Data

Depending on our relationship and interactions with you, the categories of Personal Data we process may include:

- **Contact Information** - this may include your name, title, date of birth, username, mailing address, email address, telephone number, and mobile number.
- **Identity Information** - this may include Government issued identification documentation, such as national ID, passport, your IBAN and copy of a bank statement.
- **Transaction Information** - this may include:
    - information about your transactions, including deposits, withdrawals, standing orders, scheduled transfers, description, currency, date, time, location, amount of the transaction, , payer, recipient, remittance information and information about the merchant. This may also include item-level data in some instances, and billing and shipping information;
    - information about initiated payments, including payment description, amount, currency, date, payer, recipient and registered beneficiaries; and
    - For the risk checks for our PIS we will only use the transaction history of the past 30 days, including the Transaction Information and account balance contained therein.
    - For our AIS, depending on our Partner's requested use of our Services, we can access a transaction history of up to 365 days, including the Transaction Information and account

balance contained therein. This also applies to the One-off AIS as part of our PayPlus/OnlineÜberweisenPlus Services. An exception applies to our Pay/OnlineÜberweisen Services; for these, we exclusively use the transaction history of the past 30 days for the associated One-off AIS.

- **Account Information** - this may include the name of the account holder, Bank account details (Bank account number, IBAN, sort code, BIC, Bank name and branch location, Bank account title and type (e.g. loans, mortgages, savings, investments, pensions, credit card, checking accounts), account holder type, country), account balance (including current account balance and existing account limits).
- **End User Authentication Data** - this may include the information you use to log in to your Bank, such as your Bank username, password, PIN code, email address, phone number, and the unique authentication token used to identify you as the owner of your account.
- **Inferred and Derived Information** - we infer and derive data elements by analysing Transaction Information, for determining whether the account has sufficient coverage (risk checks), security, or fraud prevention purposes.
- **Confirmation Information** - this includes the notification issued to the Partner confirming the execution status of the Service, including information on whether a transaction was initiated successfully or unsuccessfully.
- **Online and Technical Information** - this may include information about how you use our Services and your interactions with websites or applications that you use to access the Services, including IP address, date and time of access, browser type and version, operating system used, network protocols of our communication with the Bank's system, Bank user ID (only for the Continous AIS), Bank name, language, activity log records (which contain your IP address, a time stamp (date and time of the request), the requested URL and the web server processing the request), and other technical information collected when you interact with our Services.
- **Support Data** – this may include customer support dialogue and other customer communication data.
- **Compliance Data** - this includes records we maintain to demonstrate compliance with applicable laws such as the anti-money laundering checks we conduct, and records related to data subject rights requests.

Sources of Personal Data

We may collect Personal Data about you from various sources, depending on our relationship and interaction with you.

We may collect Personal Data:

- from you - (we also receive Personal Data of third parties from you, when we process the data of individuals appearing in your transactions e.g. your payors and/or payees and their Personal Data does not come to us directly but through their dealings with you);
- from Partners - depending on the Service you use, we may collect your Personal Data from Partners or service providers acting on their behalf;
- from your Bank - the Services may require us to collect Personal Data from your Bank;
- from your computer or devices - we may collect Personal Data when you use our Services on your computer or other device; and
- from our Affiliates.

Retention of Personal Data

We retain your Personal Data for as long as the information is needed for the purposes listed below and for any additional period that may be required or permitted by law. The length of time your Personal Data is retained depends on the purpose(s) for which it was collected, how it is used, and the requirements to comply with applicable laws. We retain your Personal Data when you use our Services and related services that link to this Privacy Notice in particular for the following periods:

- End User Authentication Data are only used to establish the connection to your online banking account and are not permanently stored by us. For the One-off AIS and PIS Services, such data are not retained by us. For the Continuous AIS End User Authentication Data are retained only in very limited cases, depending on your Bank's technical settings. Insofar as rention occurs for the Continuous AIS, such retention only occurs for the duration of the existing connection to your Bank and the data will be deleted after the underlying continuous connection to your Bank has been made inactive.
- Account Information, Transaction Information, Inferred and Derived Information, and Confirmation Information are generally retained for 30 days, unless certain data must be retained for a longer period for tax or commercial law reasons or for compliance with other applicable legal retention obligations (such as to comply with prevention of money laundering and terrorist financing obligations); for details see below. For the Continous AIS the data retention period begins after the underlying continuous connection to your Bank has been made inactive. For all other Services, the retention period begins from the date the respective Service was carried out.
- Activity log records are retained for 7 days. The retention period begins from the date the respective Service was carried out.
- Online and Technical Information (other than activity log records) are retained for 30 days. The retention period begins from the date the respective Service was carried out.
- Compliance Data for the prevention of money laundering and terrorist financing are retained in accordance with Art. 6 (1) (c) GDPR in conjunction with Sec. 8 (4) and Sec. 11a German Anti Money Laundering Act (GwG) for 5 years. The retention period begins at the end of the calendar year in which the business relationship ends, or in other cases, at the end of the calendar year in which the information was determined (i.e. identified and documented).
- Support Data will generally be retained only as long as needed to resolve the inquiry and handle any follow-up communication, unless statutory retention obligations apply (e.g., up to six years for business correspondence under German commercial and tax law; this retention period begins at the end of the calendar year in which the business correspondence took place).
- Personal Data required for billing purposes with the Partner and to comply with statutory retention requirements are retained for 8 years for tax or commercial law reasons, in accordance with Art. 6 (1) (c) GDPR in conjunction with Sec. 257 (1) no. 4, (4) of the German Commercial Code ("HGB") and Sec. 147 (1) no. 4, (3) of the Fiscal Code of Germany ("AO"). The retention period begins at the end of the calendar year in which the Service was carried out.

These retention periods may be exceeded if this is necessary to establish, exercise, or defend legal claims.

When it is no longer needed, the Personal Data is securely deleted or (where permitted by law) anonymized. You may request that we delete your Personal Data by visiting our website and accessing our Privacy Rights Portal or by contacting us via the details found in the "How to contact us and our Data Protection Officer" section below. If we do not have a legal basis for retaining your Personal Data, we will delete it as required by applicable law.

Why We Collect Personal Data and How We Use It

Why We Collect Personal Data and How We Use It (where you are required to provide Personal Data so that we can deliver our Services and related services, we have marked this with a *. If you do not provide the required Personal Data we will not be able to provide the respective Service or related services (such as customer support) to you)

Purpose of Processing	Categories of Personal Data	Lawful Basis and legitimate interests (to the extent that we rely on legitimate interests)
To connect to your Bank once to check your finances (One-off AIS). This includes analysing and aggregating Personal Data retrieved from your online banking account to infer and derive data, determining whether the account has sufficient coverage (risk checks), and may include sharing Account Information, Transaction Information and / or Inferred and Derived Information available to the Partner that you have chosen.	• End User Authentication Data* • Account Information* • Transaction Information* • Online and Technical Information* • Inferred and Derived Information • Confirmation Information If the Partner that you have chosen requires an overview of all accounts managed via your online banking access or if you select more than one account, the Account Information and Transaction Information for all (selected) accounts may be retrieved. Access to your online banking account is valid for 24 hours and we access your data only once.	Performance of a contract.
To connect to your Bank once to verify your name and Bank account details for an account check (One-off AIS). This includes analysing Personal Data retrieved from your online banking account for a verification of the account holder (name matching) and sharing your name and bank account details and / or	• End User Authentication Data* • Account Information* • Online and Technical Information* • Confirmation Information If the Partner that you have chosen requires an overview of all accounts managed via your online banking access or if you select more than one account, the Account Information for	Performance of a contract.

Why We Collect Personal Data and How We Use It (where you are required to provide Personal Data so that we can deliver our Services and related services, we have marked this with a *. If you do not provide the required Personal Data we will not be able to provide the respective Service or related services (such as customer support) to you)

Purpose of Processing	Categories of Personal Data	Lawful Basis and legitimate interests (to the extent that we rely on legitimate interests)
the result of the verification with the Partner that you have chosen.	all (selected) accounts may be retrieved. Access to your online banking account is valid for 24 hours and we access your data only once.	
To connect to your Bank to continuously check your finances (Continuous AIS). This includes analysing and aggregating Personal Data continuously retrieved from your online banking account to infer and derive data, determining whether the account has sufficient coverage (risk checks), and may include sharing Account Information, Transaction Information and / or Inferred and Derived Information with the Partner that you have chosen.	• End User Authentication Data* • Account Information* • Transaction Information* • Online and Technical Information* • Inferred and Derived Information • Confirmation Information If the Partner that you have chosen requires an overview of all accounts managed via your online banking access or if you select more than one account, the Account Information and Transaction Information for all (selected) accounts may be retrieved. Access to your online banking account is valid for a maximum of 180 days (depending on the technical settings of your Bank). Your data will be accessed a maximum of 4 times a day.	Performance of a contract.
For the Pay/OnlineÜberweisen Service: To connect to your Bank once to make your payment (PIS).	• End User Authentication Data* • Account Information* • Transaction Information*	Performance of a contract.

Why We Collect Personal Data and How We Use It (where you are required to provide Personal Data so that we can deliver our Services and related services, we have marked this with a *. If you do not provide the required Personal Data we will not be able to provide the respective Service or related services (such as customer support) to you)

Purpose of Processing	Categories of Personal Data	Lawful Basis and legitimate interests (to the extent that we rely on legitimate interests)
Before the payment, we will also carry out an account information service on a one-time basis to check your finances first (One-off AIS). This includes analysing and aggregating Personal Data retrieved from your online banking account to infer and derive data and determining whether the account has sufficient coverage (risk checks). We will only share a payment confirmation with the Partner that you have chosen.	• Online and Technical Information* • Inferred and Derived Information • Confirmation Information Access to your online banking account is valid for 24 hours and we access your data only once.	
For the PayPlus/OnlineÜberweisenPlus Service: To connect to your Bank once to make your payment (PIS) and share your financial information with our Partners. Before the payment, we will also carry out an account information service on a one-time basis to check your finances (One-off AIS). This includes analysing and aggregating Personal Data retrieved from your online banking account to infer and derive data and determining whether the	• End User Authentication Data* • Account Information* • Transaction Information* • Online and Technical Information* • Inferred and Derived Information • Confirmation Information Access to your online banking account is valid for 24 hours and we access your data only once.	Performance of a contract.

Why We Collect Personal Data and How We Use It (where you are required to provide Personal Data so that we can deliver our Services and related services, we have marked this with a *. If you do not provide the required Personal Data we will not be able to provide the respective Service or related services (such as customer support) to you)

Purpose of Processing	Categories of Personal Data	Lawful Basis and legitimate interests (to the extent that we rely on legitimate interests)
account has sufficient coverage (risk checks). After the payment was initiated, we will share Account Information, Transaction Information, Inferred and Derived Information and a payment confirmation with the Partner that you have chosen.		
Provide customer support to you or Partners in connection with our Services.	• Identity Information* • Contact Information* • Support Data*	Our legitimate Interests to maintain appropriate standards of service.
To comply with applicable laws regarding our Services (including security, statutory retention requirements, anti-money laundering requirements, know your customer requirements, requirements on incident management, fraud prevention, consent management, and responding to data subject rights requests).	• Contact Information* • Identity Information* • Account Information* • Transaction Information* • Online and Technical Information* • Inferred and Derived Information • Confirmation Information • Support Data • Compliance Data Where compliance with these obligations involves the processing of criminal offence data (e.g. when we are performing anti money laundering and terrorist financing checks), we only conduct such processing where permitted by local law.	Compliance with our legal obligations.

Why We Collect Personal Data and How We Use It (where you are required to provide Personal Data so that we can deliver our Services and related services, we have marked this with a *. If you do not provide the required Personal Data we will not be able to provide the respective Service or related services (such as customer support) to you)

Purpose of Processing	Categories of Personal Data	Lawful Basis and legitimate interests (to the extent that we rely on legitimate interests)
For security purposes (e.g. identification and blocking of DDoS attacks), we will store activity log records.	• Online and Technical Information*	Our legitimate interests to ensure trouble-free operation of our Services and related services and thus also the protection of Personal Data.
To ensure the effective running of our business including processing as necessary for the purposes of (i) enforcement of contracts; (ii) contract management; (iii) account management; (iv) quality control; (v) fraud prevention; (vi) corporate governance; (vii) reporting; and (viii) disaster recovery and business continuity.	• Identity Information • Contact Information • Account Information • Transaction Information • Online and Technical Information • Inferred and Derived Information • Compliance Data	Our legitimate interests to ensure the efficient, secure, and reliable operation of our business, the protection of End Users, Partners and systems, and our ability to meet internal governance, accountability, and operational standards.

Why We Collect Personal Data and How We Use It (where you are required to provide Personal Data so that we can deliver our Services and related services, we have marked this with a *. If you do not provide the required Personal Data we will not be able to provide the respective Service or related services (such as customer support) to you)

Purpose of Processing	Categories of Personal Data	Lawful Basis and legitimate interests (to the extent that we rely on legitimate interests)
For product development and enhancement and troubleshooting: • generate anonymized datasets which are used for product development and enhancement, and troubleshooting, incuding aggregated datasets that are anonymous; • understand how you and others use our Services, for analytics and modelling and to create business intelligence and insights and to understand economic trends; and • preference management and providing product updates.	• Account Information • Transaction Information • Inferred and Derived Information • Online and Technical Information	Our legitimate interests to perform analysis and take steps to aid the progression of our business.

Why We Collect Personal Data and How We Use It (where you are required to provide Personal Data so that we can deliver our Services and related services, we have marked this with a *. If you do not provide the required Personal Data we will not be able to provide the respective Service or related services (such as customer support) to you)

Purpose of Processing	Categories of Personal Data	Lawful Basis and legitimate interests (to the extent that we rely on legitimate interests)
Safeguarding our rights	• Contact Information • Identity Information • Transaction Information • Account Information • Inferred and Derived Information • Confirmation Information • Online and Technical Information • Support Data • Compliance Data	Our legitimate interests to establish, exercise and/or defend legal claims.
To manage and/or administer the sale of our business or any assets (including mergers, acquisitions and divestitures).	• Contact Information • Identity Information • Account Information • Transaction Information • Inferred and Derived Information • Online and Technical Information • Confirmation Information • Support Data • Compliance Data	Our legitimate interests to conduct and complete corporate transactions efficiently and lawfully, ensure the accurate assessment of the business or assets being sold, and allow for the continuation of operations and relationships through and after such transactions.

Categories of Third Parties and Our Disclosure of Personal Data

Your Personal Data is primarily shared with the Partner whose servicesyou utilize and whom you have instructed us to make the data accessible to.

Your Personal Data may also be shared with:

- our Affiliates, which are companies related by common ownership or control, including Tink A.B. and other companies of the Visa group;
- your Bank when you request that we provide our Services. The End User Authentication Data you have shared with us are only disclosed to your Bank and only when the respective Services are performed.
- Partners and Banks (or their authorised processors), for the purposes of providing Services to you, managing fraud and risk, and supporting the purposes outlined in the table above;
- regulators and other authorities (including law enforcement authorities such as the police or the Financial Intelligence Unit - FIU) to comply with our legal obligations or investigations, or to safeguard our rights;
- courts, other parties to a litigation and our professional advisors; and
- our service providers, such as software and data storage providers who process your Personal Data on our behalf and strictly in accordance with our instructions. We use the follwoing processors to provide our services:

    - Uvensys GmbH, Robert-Bosch-Straße 4b, 35440 Linden, Germany. Description of processing: Managed hosting of servers (including firewall and DDoS protection).
    - Cloudflare Inc., 101 Townsend Street, San Francisco, CA 94107, USA (Cloudflare participates in the EU-U.S. Data Privacy Framework and thus provides an adequate level of data protection; see also the section “International Transfers”). Description of processing: Provision of a web application firewall solution.
    - Tink AB, Vasagatan 11, 111 20 Stockholm, Sweden. Description of processing: Supporting services, in particular customer support.

We may disclose Personal Data with other third parties with your consent, or as permitted by law, such as when we sell or transfer business assets, enforce our contracts, protect our property or the rights, property or safety of others, or as needed for audits, compliance, and corporate governance.

Profiling and Automated Decision-Making

“**Profiling**” is any form of automated processing of Personal Data consisting of the use of such Personal Data to evaluate certain personal aspects relating to a natural person, such as to analyze or predict aspects concerning that natural person’s economic situation.

“**Automated decision-making**” is when automated means without human intervention are used for making a decision in relation to an individual, such as denying an individual to use a service.

We may use profiling when processing your Personal Data in connection with our Services. We may also use automated decision-making, including profiling, when processing your Personal

Data in connection with providing our PIS. For this Service we use your Personal Data for automatically determining whether a payment will be initiated based on risk checks carried out to determine whether your account has sufficient coverage. For instance, we may assess the amounts and volumes of your transactions based on your account in relation to a Partner and whether your initiated payments in relation to a Partner were successfully executed. Depending on the results of the risks checks, the payment will either be initiated or not initiated by us.

We will not make automated individual decision-making about you, including profiling, which produces legal effects concerning you or may similarly significantly affect you.

Your Privacy Rights

By law you have a number of rights. You can submit requests under relevant laws to us via the details found in the "How to contact us and our Data Protection Officer" section below.

These rights may include to:

- **Request access to your Personal Data**

  We will then provide you withe a copy of the Personal Data we hold about you so that you can check that we are lawfully processing it.

- **Require us to change incorrect or incomplete Personal Data**

- **Require us to delete your Personal Data**

  This enables you to ask us to delete or remove Personal Data where there is no good reason for us continuing to process it, you have withdrawn your consent, you have exercised your right to object to processing and there are no overriding legitimate grounds for us to continue doing so, the Personal Data has been processed unlawfully or we are legally required to delete it. This does not apply e.g. where we need to process the data to establish, exercise or defend a claim.

- **Require the restriction of the processing**

  In cases where the accuracy of your Personal Data is contested (for a period enabling us to verify the accuracy of the Personal Data), the processing is unlawful and you oppose our use of the data and ask it to be restricted, where you have objected to the processing of your Personal Data and are awaiting our assessment of whether we have overriding legitimate grounds to continue processing it, or that we no longer need the Personal Data but you need it for legal claims purposes, you may ask for the restriction of the processing of such Personal Data. This means that Personal Data will, with the exception of storage, only be processed with your consent, for the establishment, exercise or defence of legal claims, for the protection of the rights of another natural or legal person, or for reasons of important public interest. Where processing is restricted, you will be informed before the restriction on processing is lifted.

- **Withdraw your consent under data protection law (in the limited circumstances where you may have provided consent)**

  You have the right to withdraw your consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. The withdrawal only affects future processing.

- **Object to the processing of your Personal Data**

  You may object, on grounds relating to your particular situation, to processing which is based on the legitimate interests pursued by us or by a third party. In such a case we will no longer process your Personal Data unless we have compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

- **Require data portability**

  Where automated processing of your Personal Data is based on consent or the execution of a contract with you, you also have the right to data portability for information you provided to us – this means that you can obtain a copy of your Personal Data in a commonly used electronic format so that you can manage and transmit it to another data controller.

- **Lodge a complaint**

  You also have the right to lodge a complaint with a data protection supervisory authority. If you have any concerns about how we process your Personal Data, you are entitled to lodge a complaint. We encourage you to contact us first so we can address your concerns directly. Please contact us using the contact details below. We take all complaints seriously and will respond as promptly as possible.

Generally, you will not have to pay a fee to access your Personal Data (or to exercise any of the other rights). However, where permitted by law, we may charge a reasonable fee, for example if arequest for access is clearly unfounded or excessive. You may be required to provide additional information which verify your identity before we can respond to your request.

International Transfers

We may transfer your Personal Data between countries, including to countries which may not have similar privacy or data protection laws as your country of origin. However, we will always protect your information and transfer it in accordance with any applicable legal requirements for cross-border transfers of Personal Data. Where Personal Data is transferred to the United States from Europe, we will verify if the recipient ensures an adequate level of protection by participating in the EU-U.S. Data Privacy Framework. If this is not the case, or if Personal Data is otherwise transferred outside of the EEA, we will ensure it is protected by other appropriate safeguards, such as Binding Corporate Rules, the EU Standard Contractual Clauses approved by the European Commission, or other legally permitted mechanisms, to ensure that the level of data protection afforded in the EEA is not undermined. You may obtain a copy of such safeguards by using the contact details below.

Information Security

We take the security of your Personal Data seriously. We use physical, technical, organizational, and administrative safeguards to help protect your Personal Data from unauthorized access or loss. For example, we use encryption and other tools to protect sensitive information. Where we engage third parties to process Personal Data on our behalf, they do so on the basis of written instructions and have a legal requirement to implement appropriate technical and organisational measures to ensure the security of Personal Data in compliance with the applicable data protection laws.

Changes to this Privacy Notice

We will make changes to this Privacy Notice from time to time. For example, we may make changes to this Privacy Notice to keep it up to date or to comply with legal requirements or due to changes in the way we operate our business. Any changes or updates we may make will be posted on our website so that you are aware of the impact to our data processing activities before you continue to engage with us.Please check back frequently to see the latest version on our website.

How to Contact Us and our Data Protection Officer

If you would like to exercise your privacy rights (with the exception of the right to lodge a complaint with a data protection supervisory authority), please visit the Privacy Rights Portal or contact us as described below.

If you would like to contact our Data Protection Officer, please send an email to datenschutz@tink.com or a postal letter using our contact details stated below. Please always include the addition "*(personally) to the data protection officer*" to your message.

For any other assistance, or to exercise your rights (including your privacy rights and other rights as an End User), you may contact us at the information below (*Please do not include sensitive information, such as your account number or a copy of your ID, in emails*):

- Email us: contact@tink.com
- Write to us:

  Tink Germany GmbH

  Gottfried-Keller-Strasse 33

  81245 Munich, Germany